December ___, 2014

Caleo Health
#200, 1402 8 Avenue NW
Calgary, AB T2N 1B9
Ph: 403-452-0999; Fax: 403-984-5448

Ms. Jill Clayton, Commissioner
Office of the Information and Privacy Commissioner
# 410, 9925 - 109 Street
Edmonton, Alberta
T5K 2J8

**RE: Privacy Impact Assessment – Update Submission to Our PIA for Brightsquid Secure EMR System – Caleo Health**

Dear Ms. Clayton:

Please accept our Organizational and System Privacy Impact Assessment (PIA) update to our existing submission (H# 5264, accepted January 22, 2013) for your review. I am submitting the enclosed documents in compliance with section 64 of Alberta's *Health Information Act* (*HIA).*

Clinics and custodians are expected to use the most secure means possible to communicate with patients and other custodians in their role as health care providers when discussing case management, setting up appointments, and for other related communications involving the patient's identifiable health information. While OIPC has provided guidance for general email use in managing patient appointments in the same manner as voice mail might be used (OIPC HIA Practice Note #5, dated August 2012), this communications is limited to appointment related information only. Where more detailed patient health information needs to be exchanged, a higher bar of expectation is set for health information safety and security for such exchanges, and regular email is generally acknowledged as not providing enough security for such.

I am submitting this PIA update for our clinic and custodians (as listed in our existing PIA) using a non-streamlined process for participation in use of a new information collection and handling capability at our clinic related to the above identified purpose. This new capability is a secure email service provided by Brightsquid Dental Ltd based out of Calgary, Alberta. The system provides an encrypted Web-based interface for a secure email portal to exchange sensitive messages and documents in a safe and secure environment while also providing the ability to provide non-sensitive message components and notices of waiting sensitive messages to users by general email. This combines the benefits of a secure environment for those portions of the message and attached documents sensitive to disclosure while at the same time allowing the leveraging of general email's widespread pervasiveness on all devices and in all parts of the Internet to ensure timely general communications combined with timely notice of sensitive messaging/documents waiting.

This new secure email system allows the sharing of identifying health information in a secure environment, a capability currently not provided by regular email programs and protocols. The disclosure of identifying health information to other custodians for purposes of continuing care and provision of health services and communicating such information to and receiving such information from the patients to enable same are covered under the collection, use, and disclosure provisions of the *HIA*. But because this collection, use, and disclosure through communications is carried out in a new manner for our clinic using new information handling tools that involves partnering with a new vendor/service provider, we are submitting this update PIA as required by the *HIA* for review and feedback by OIPC to ensure best practices are being followed and potential risks involved have been properly considered.

This update PIA is a supplement to our existing PIA and involves new details related to existing administrative, technical, and physical safeguards for information handling, safety, and security. It however requires no changes to our existing Privacy and Security policies and procedures, instead referencing and using policies and procedures already in existence. We anticipate any amplification to these procedures and safeguards will be covered fully by this submission.

We are also using this update cover letter to report a change in location for our clinic, from our old location on Crowfoot Crescent in Calgary to the new address in this letter and PIA submission. The new location is a medical office centre managed by Alberta Health (former hospital site). Our entrances, general spaces, security measures, and administrative, technical, and physical safeguards remain the same in our new location as per our original PIA submission. Wired and wireless networking connections continue to be used, with wireless networking being set up by our vendor in accordance with VCUR 2008 and Netcare standards. The move had no impact on health information handling as we employ a VCUR 2008 compliant ASP hosted EMR system as per our original PIA quoted in this submission.

Custodians participating in this update PIA submission include:

Dr Jacques Bouchard
Dr Cory Cundal
Dr Ganesh Swamy
Dr Peter Lewkonia
Dr Stephan du Plessis
Dr Alex Soroceanu
Dr Arun Gupta
Dr Denise Bowman
Dr Michael Christie
Dr Scott Wilson
Dr Joanne Storring (chiropractor on staff)
Dr Francine van Rooyen
Dr Caeley Lorincz

Dr Roger Cho
Dr Richard Hu
Dr Ken Thomas
Dr Paul Duffy
Dr Deon Louw
Dr Mark Lewis
Dr Tony Glantomaso
Dr Wilhelm Meerholz
Dr Christopher Morse
Dr Elias Soumbasis
Dr Philip Braithwaite
Dr Frederick van Rooyen

I trust that this will be satisfactory.

Sincerely,

Dr Richard Hu
Lead Custodian

| | |
|---|---|
| Enclosures: | Privacy Impact Assessment |
| | Risk Assessment Table |
| | Interface Screen Shot |

# PRIVACY IMPACT ASSESSMENT

## Organization Management
## and
## Organization Medical Information Communications System
## (Brightsquid Secure Email System)

**Caleo Health**

Dr RIchard Hu
**Clinical Director / Lead Physician**

Dr Mark Lewis
**Privacy Officer**

**Clinic Name:** Caleo Health

**Legal Name of Lead Custodian or Organization:** 1344417 AB Ltd

*Contact Information:*

Dr Mark Lewis, Clinic Privacy Officer
Caleo Health
#200, 1402 8 Avenue NW
Calgary, AB T2N 1B9
Canada

Phone: 403-452-0999
Fax: 403-984-5448
Email: MarkLewis@caleohealth.ca

PIA Submission Date: December 5, 2014

Previous PIA Submission:
☐ No ☒ Yes - H# 5264 Acceptance date: January 22, 2013

Changes since previous PIA submission:

- Implementation of a secure email system for communicating sensitive information and documents with other custodians, staff, and patients.

Version Control

| Date | Version | Author of changes | Description |
|---|---|---|---|
| December 5, 2014 | 1.0 | Privacy Officer | Original draft |
| | | | |
| | | | |
| | | | |

# Table of Contents

# Section A: Project Summary

Caleo Health is a medical clinic providing family medicine and multidisciplinary spinal-related consultation and treatment services to all patient demographics in the Calgary area as reported in our existing PIA.  In order to provide care, the clinic must collect, use and disclosure health information.

## Project Background

Caleo Health is filing this update Privacy Impact Assessment (PIA) to remain in compliance with Section 64 of the Alberta *Health Information Act* (*HIA*).  All custodians are required to report on updates to their information safety and security practices when it comes to personal health information they have in their care and custody.  This is a key step in demonstrating willful compliance with the provisions of the *HIA* and related legislation.

Further to this, participating in the PIA process and having the organization's update PIA accepted by the Office of the Information and Privacy Commissioner demonstrates that our custodian(s) follow good information safety and security practices including having an active program to improve these practices as we become aware of new trends and ideas going forward.  This demonstration of good practices in turn opens the door to partnering with organizations and applying for services that require some form of proof that the clinic has such measures in place.

For this update PIA, we are initiating a project related to secure email/messaging services through a new service provider.  This service is aimed to improve communications between custodians providing health services including referrals/consults as permitted by Section 35 of the *HIA* as well as communications between patients and custodians.  Further, this capability is being initiated to both improve timeliness of contact and exchange of information and security of same.

Identifying health information can be regarded as anything pointing to the identity of the person combined with any element that can identify the nature of health services the person is receiving such as medical chart information.

Custodians are obligated to maintain the privacy and confidentiality of identifying health information to the greatest extent possible within reason as part of collecting, using, storing, disclosing, and disposing of said information in the course of providing health services and carrying out duties and responsibilities related to same or as necessitated by obligations under, for example, legislation or professional guidelines.

The *HIA* identifies a custodian's obligation under Section 60(1) to take reasonable steps to protect the confidentiality of health information in their custody including maintaining administrative, technical, and physical safeguards to provide this protection. Section 60(2)(a) further requires that these safeguards include appropriate measures for the security and confidentiality of these records.

In the recent past, as identified by OIPC HIA Practice Note #5 (dated August 2012), acceptable communications practices have expanded to include use of email for basic functions such as appointment management.  This does potentially expose the identity of the person as well as what service provider and potentially, by inference or appointment details such as preparation requirements, the nature of medical service to be received. However, when properly managed using a patient-provided and confirmed email address as identified in the OIPC HIA Practice Note quoted, such communications can be considered as reasonably secure as using voice mail for limited types of information such as appointment scheduling at a patient-provided and confirmed phone number.

In the same vein, faxing of information carries risks similar to voice mail and general email where successful receipt in a secure and private manner is heavily dependent on the accuracy of fax phone number information provided by the receiving agency directly or by the patient. There is further risk from the fact that faxed copies of information can also be of varying quality, risking loss or limiting the usefulness of the information for provision of health care services or other allowable purposes as identified by applicable legislation.

With the above considerations in mind, we are undertaking to employ a new secure email service provided by Brightsquid Dental Ltd, an Alberta based company, that includes a secure messaging and secure document delivery component through an encrypted Web portal. This portal is compatible with desktop and mobile browsers including on smart phones. Accounts exist for primary custodians as a paid service, with an associated number of subordinate affiliate accounts and unlimited number of patient accounts. The interface scales to the screen size used for access.

Custodian accounts have the ability to invite new subordinate users and manage the contact list, while subordinate affiliate accounts can invite new health care providers to the system to receive a communication on behalf of custodians or invite patients to receive a communication. Patient user invites include the ability to validate the identity of the patient receiving the communication (requirement of person receiving invite to enter their birth date to compare against data entered into the invite at the server level by sending user…the actual date entered by the sending user is never displayed to the person receiving the invite). There is no validation step for health care provider level new user invites as there is a reasonable baseline assumption similar to fax number use that the user sending the invite has verified that the email address the invite is being sent to is associated with the health care provider who is being invited to set up an account and receive a communication.

The Web interface for users provides access to the appropriate contact list for user types. An individual contact record includes regular email address for receiving message notifications, user name/identity as entered by the person inviting a new user and eventually as updated by the invited user as their public-facing identity information. Users overall can only see the contacts that are associated with their group (practice/clinic), while clinic associated accounts can see other health care practitioners in the system off a successful search by identity or regular email address. A user can be in multiple contact lists but the only commonality linking them to the user is the email address and identity name. Internal contact lists allow for users to enter commentary type information associated with the contact, but this will not appear in other lists or to the user who is the contact. At the same time, the user identified in a contact can enter public facing information to enhance their profile for identity and contact purposes.

The user Web interface also provides two fields for messaging, one for the unsecure component capable of going to the receiving user’s regular email address along with notifications of secure messages/documents, and one for a secure messaging component where information that can only be viewed from within the secure Web portal after login can be entered. Finally, there is a field area for attachment of documents and files for either downloading from the site or viewing within it if an appropriate viewing capability is available within the version of the system in use at that time (currently restricted to image files only, expansion to other file types being considered). The viewer even allows users to insert comments/annotations on viewed files to be re-saved and sent back to the sending user.  Up to 500MB of files can be attached by a user to a message. This along with other tools provided by the interface allows for collaborative work between custodians and/or clinics within a secure environment without ever having to download the file to view or use until such time as work is complete (currently restricted to supported viewable file types only). This collaboration is carried out in accordance with Sections 27(1)(a) and 35(1)(a and b) of the *HIA*, with the secure email system simply providing another means similar to mail, fax, and phone collaboration methods but all within a secure back-and-forth communications environment.

User account management is carried out through custodian user accounts or designated subordinate user accounts identified to perform this function.  This includes a user profile management system to set up names, contact information, pictures of users if desired, and other notes and details as desired to enable other users to clearly identify a specific profile. Users are grouped by custodian account and below or, for larger user groups, by clinic/practice and below where several custodian user accounts are involved.  Custodians and subordinate users can see all users' public-facing identity information within the overall product domain and search them accordingly. Patient users can only see the user group (custodian or clinic/practice) inviting them to create an account, for communications with that group and/or subsequent groups only (i.e. after communicating with the first clinic to invite them to the secure email system, a new clinic they go to invites them to communicate with that group too). Patient accounts for user groups are free and unlimited; encouraging user groups to make use of the system for their patient population at large rather than restricting this usage and further promoting secure communications between health care providers and patients over use of regular email communications.

The system is managed from Calgary, Alberta by Brightsquid.  It is hosted on servers that are part of a Tier 2 data centre run by Peer1 as a subcontractor to Brightsquid in Markham, Ontario. The data centre has the appropriate measures as described later in this PIA to provide for system and data safety and security.  Brightsquid has undertaken to ensure significant layers of fail-over redundancy are built into the system equipment and support involved through the data centre.  Brightsquid as primary contractor has appropriate security and confidentiality agreements in place with the data centre as sub-contractor for hardware, software, and data safety and security management.

Our eventual goal is to reach a status where employing this system presents minimal risk to personal medical information while enabling an improved communications experience for custodians, staff, and patients in the clinical environment.  We shall endeavor to further describe the approach planned and related safety and security factors as part of this PIA.

The clinic physicians, as individual custodians of health information, have undertaken reasonable steps to maintain administrative, technical, and physical safeguards to protect the confidentiality of the information under our custody and control including when used for health service provider education.  As custodians under the *HIA*, physicians are required to protect the health information in their custody or control against **reasonably anticipated threats or hazards** that could result in loss, unauthorized disclosure or use, modification or inaccuracy.

This update PIA submission is documentation of the reasonably anticipated threats or hazards, and (of the suitable) safeguards put in place by Dr RIchard Hu, as Lead Physician for the organization, to manage those threats and hazards in the organization's use of this new capability.

## Clinic Profile

| | |
|---|---|
| Clinic Address: | #200, 1402 8 Avenue NW<br>Calgary, AB T2N 1B9<br>Ph: 403-452-0999; Fax: 403-984-5448 |
| Clinic Privacy Officer: | Dr Mark Lewis, Clinic Director |
| Type of Clinic: | The clinic provides family medicine and multidisciplinary spinal-related consultation and treatment services to all patient demographics in the Calgary area. |

Please see Section A or equivalent of our existing PIA for more details on the clinic organization and related existing information systems.

# Section B: Organizational Privacy Management

Please see our existing PIA for details on our clinic organization including management structure, policy management, training and awareness, and incident response.

## Project Management Structure and Agreements

Caleo Health is engaging the services of a new vendor for a new information handling service related to secure communications. This is a secure email or messaging service provided by Brightsquid Dental Ltd based out of Calgary, Alberta. The system will be referred to as the secure messaging system or the secure messaging service and the company will be referred to as Brightsquid for the remainder of this PIA for brevity and clarity purposes.

The management structure for this project is a customer-to-vendor/service provider relationship with the clinic being the customer and Brightsquid the service provider. Brightsquid as service provider in turn is responsible to custodians as customers for the provision of service and any related system and staff matters involved in providing this service and its usage in relation to health information as well as impacts to it on behalf of custodians.

Because the service provider does not have access to user accounts and information through the system administration tools, it is not possible for staff to view personal health info or private communications directly even with user involvement. Brightsquid staff level of access is to be to enable or disable accounts and to force password changes only. As such, the vendor is instead providing a more traditional role of system manager rather than direct management of the information within the system.

This relationship is in the custodians view is technically a non-information manager relationship similar to telecommunications and email service providers where the vendor has no normal direct access or direct hands-on role in managing the information within user accounts in the system. This does not necessarily make this sort of service provider a non-information manager (IM) in the eyes of the *HIA* and OIPC though unless the mischief approach to legislation interpretation is employed instead of literal interpretation alone. As such, it remains the responsibility to ensure either a direct IM relationship is entered into through a traditional IMA, or to ensure the provisions expected of an IMA are part of a public-facing service agreement or equivalent public service promise that meets the same requirements.

This second option is more likely for such a service as the majority of information portal and information pass-through services in today’s cloud computing environment involve a non-paper “signup for service” process who’s workflow do not permit mail or other such exchange of signature steps in the traditional sense. Further, a delay for signatures would impede the purpose of inviting patient or non-user health care providers to receive a communication in an easy manner that permits timely provision of health care services that may be important to a particular treatment need. Finally, few if any health care providers or patients are set up with certified digital signature products attuned to a common public standard that can easily be used to authenticate agreement to terms of use and privacy and security commitments.

As such, instead a service provider in today’s electronic environment has to be ready to implement alternate means to make their privacy and security commitments available to custodians and patients as users in a readily apparent manner. This approach permits custodians to meet their responsibility to review a service provider for appropriate measures and commitments to user information privacy and security.

The vendor as an Alberta-based company focused on providing secure communications related services to health service providers in the province as well as national and international clients, has made an active commitment to providing service promises that reflect both the Alberta *HIA* and *HIPAA* compliance expectations as laid out by the United States for covered entities and services supporting them. The company expresses these commitments through its user privacy and security statement and terms of use statement that are available in full form at user initial signup for service and through Web links embedded in the user login and main interface pages available for review by users at any time. The users at signup are asked to review these terms and commitments and click on a positive acknowledgement that they have had this information made available to them for review.

Further towards proving their commitment to health information privacy and security, the vendor company has embarked on obtaining a certification of HIPAA compliance for their company and products including the secure messaging system and setting up an accreditation process for maintaining this compliance with annual reviews in accordance with US laws. Again, the status of this compliance accreditation is made available to potential and existing users through the company's Website and user login page.

The custodians have reviewed the privacy and security and terms of use statements, and ensured to the best of their ability that they are structured to reflect Sections 7.2 and 8.4 of the Alberta *HIA Regulation* and HIPAA requirements covering safe use and storage of information for users and proper notification to users of breaches or concerns. The service provider company further regularly reviews legislation to ensure these provisions are up-to-date while still reflecting reasonable expectations for service providers and worded to cover the multi-jurisdictional nature of the company's clientele.

## Project Policy Management

Our clinic has a set of health information privacy and security policies and procedures that specifically addresses privacy protection and includes a Privacy Charter and policies covering collection, use, disclosure, access, and information safety and security. These policies and procedures were provided as part of our existing PIA submission and should be referenced for any questions related to standing policy and procedure within the clinic.

Clinic use, disclosure, and protection of health information as part of communications with patients and referral/consult/collaboration related communications between health care providers are governed by existing clinic policies and procedures. The implementation of a secure messaging service is regarded as an extension of and improvement to the tools used for these communications activities.

To ensure compliance by staff and custodians using the new system within these existing policies and procedures, the clinic employs the following additional steps either directly or in conjunction with the vendor company:

- Training of staff on use of system interface fields for messages including what is acceptable information that can be entered into the unsecure field that will be forwarded to recipients' regular email and what types of information must be sent via the secure

information field and/or secure document attachments. This training is in-line with the *HIA* and OIPC HIA Practice Note #5 on email usage as well as internal clinic privacy and security policies.
- The secure messaging system provides reminders on acceptable use of the unsecure information field in terms of use and ensuring correct addressee in the form of reminder banners, privacy and security statements and reminders within interface fields and bodies of messages, and as links to policies in the user interface.

The custodians involved in this update PIA submission are also responsible to examine the privacy policies and health information safety and security standards of the service provider (Brightsquid) to satisfy themselves that appropriate safeguards and measures are in place to protect personal health information shared between staff and with other health care providers using the secure messaging system.

Specific details about the service provider's privacy policies and measures identified include:

- The service provider has appropriate internal information privacy and security policies concerning information in their care and custody.
- The secure messaging system is implemented so that company staff have no direct access to information in user accounts through system administration tools and the database is encrypted at rest. The database developer in theory has the ability to access the raw database containing user information in the course of troubleshooting or upgrading the system. Such access events require company management permission though, and are monitored by an independent audit log system to track access to the core database at rest. The database manager has a signed confidentiality agreement in place with the company, and only management has access to the audit logs to ensure database developer compliance with the terms and conditions of this agreement.
- Messages sent to non-system users will generate a notification email along with info from the unsecure information field to the intended recipient inviting them to sign up to the Brightsquid system as a free user (i.e. patient), walking them through the signup and proper usage notification process, and finally allowing them to access the secure message sent to them in a safe environment with appropriate user reminders within the interface to proper usage. The email address used to send out notifications of waiting messages is one-way only and does not accept return emails, limiting the risk of invited or regular users trying to use regular email to respond with sensitive information. Any such emails are instead rejected and "bounce back" to the person sending the reply. Replies can only be sent from within the secure messaging system.
- The system provides the ability for users sending messages to review outstanding invitations to establish an account and sign in to retrieve messages sent to non-system users (colleagues and patients) to ensure no information is lost due to lack of notification of successful delivery or inability to review information delivery status for messages that involve invitations to the system.
- For colleagues, there is an expectation that users will have the right email address to reach other health care providers that are non-system users. This expectation is in line with expectation for using a fax to send health information to another health care provider. For patients, the secure messaging system requires that the custodian or staff member inviting a patient to create an account to enter the patient's birth date as part of the invite verification data. The system sends an invite that includes a secure link in the email to the patient. This link takes them to an encrypted Web page for account creation.

This page requires the patient to enter their birth date as an identity-verification step, which is compared to the date entered by the staff/custodian inviting the patient.

## Training and Awareness

### Clinic Privacy Training

The clinic custodians, directly or through the clinic Privacy Officer, are responsible to ensure that clinic staff are familiar with and trained in the clinic's privacy and information safety and security practices in accordance with the clinic's existing Privacy policies and procedures as required by Section 8(6) of the *HIA Reg*.

The service provider is responsible for their own staff training in privacy and security matters in accordance with the information provided to custodians during their review of the company to determine if they were a suitable vendor for providing secure communications services to the clinic.

Upon request, the vendor is responsible to make its privacy policies and practices available to participating custodians for review in accordance with the custodians' obligations under Section 8(3) of the *HIA Reg*. The vendor is proactive in this matter, providing both terms of use and privacy and security policies through links on its login and main interface pages.

### System Privacy Training and Awareness

The secure messaging system is a version of an email messaging service where the vendor's general staff by policy does not and/or by system design is unable to access user accounts to manage information contained therein on behalf of users. Despite this, the vendor does undertake privacy and security training with staff with a focus on health information handling best practices and maintains this training on an annual basis. Further, employees are expected to sign confidentiality oaths with the vendor that includes references to protection of client information.

Custodians are able to view information on privacy policies and statements and related health information safety and security measures as provided by the vendor through the vendor Website and system user interface to meet a reasonable bar of disclosure and transparency expectations and adequately demonstrate that the company has good policies in place and company staff are appropriately trained in privacy and security for managing the system on behalf of customers using the service.

User training on safe use of the service for secure messaging to health care providers and patients is carried out through a combination of two measures. One is in-clinic measures (in compliance with best practices such as OIPC HIA Practice Note #5 and clinic internal policies and procedures as reported in our original PIA submission) to ensure user awareness of policies and procedures in accordance with *HIA Reg* Section 8(6) requirements.  The second is in-system user training and reminder prompts provided by the system as described in this PIA submission. The custodians regard this as a suitable level of user training and awareness for use of the secure messaging system by staff and patients signing up for the system.

# Incident Response

## Privacy Breach Management

Privacy breaches identified by the custodians and/or their affiliates are managed in accordance with the clinic's current privacy and security policies and procedures as outlined in our existing PIA.

IT Related Service Providers

Brightsquid as the system service provider/vendor with minimal access to user account information except in limited circumstances with the database developer, has identified its breach risks are more directly related to system hacking that might restrict access to information more.  Because of the database's nature of being encrypted at rest, compromise of data is monitored for but is a lower risk.

Brightsquid responds to personal information safety and security breaches in a similar manner as other IT companies. The company immediately notifies affected account users of technical or physical breaches of accounts preventing access or compromising information contained therein once the breach is detected, in accordance with company policies and service agreements. The company takes all reasonable steps to re-secure accounts and the system, rectify any identified shortcomings in safeguards that may have contributed to the breach, and mitigate damage to user account safeguards and accounts immediately and on an ongoing basis as required.  In turn it is the company's responsibility to require the same measures and responses of any of its suppliers or contractors on behalf of system users and their accounts.

As previously stated though, the company does not have regular access to information within accounts, and it is therefore the responsibility of users to determine the nature of information breached and impact thereof in accordance with their own policies and procedures and legislation affecting the information involved.

## Access and Correction Requests

Requests for access and correction to personal health information in the care of clinic custodians are dealt with in accordance with existing clinic privacy and security policies as submitted in our existing PIA.

IT Related Service Providers

As the company and its staff have no regular access to patient information through system administrative tools, any requests for access to information or correction cannot be actioned directly by Brightsquid staff.

The company instead advises those making such requests that

- It will forward such requests to the users affected if able to based on the information provided by the requester to identify the relevant users involved;
- That the company itself has no regular access to this information and therefore cannot provide it; and

- That the company cannot give out user identities and contact information to requesters in respect for user privacy and security rights under local legislation unless requesters have clearly identified the parties involved themselves or in responding to a lawful court order for the relevant jurisdictions involved.

# Section C: Project Privacy Analysis

## Project Health Information Listing

The contents available in a secure messaging system can include any and all information that is potentially contained in a patient chart with due regard for expressed wishes and other related restrictions for patient confidentiality, privacy, and safety purposes as allowed under professional standards for health professions and applicable privacy legislation.

This system is not intended as a replacement for the patient chart though some collaboration related communications between health care providers can occur over it.  As such, it remains the custodians' responsibility to ensure important personal health information as updated for collaboration within the secure messaging system is included in charts and is not lost.

Communications using the system may include the following personal health information:

Registration information
The communications will usually need to identify the patient involved when said communications is between health care providers and needs to reference the patient for context purposes.

The communications will also need to refer to the patient's identity by default when using the secure messaging system to communicate between health care provider and patient directly.

Patient identity information can include name, address, contact information, personal health number, and any other such registration information relevant to facilitating the communication's conversation between health care providers or between a health care provider and patient.

Diagnostic, treatment, and care information
Medical history or diagnostics/care information may be included as part of targeted communications between health care providers or between health care providers and patients over a secure messaging system such as the one detailed in this PIA. The type of information included will depend entirely upon the nature of the communications just the same as a phone conversation or fax conversation between providers or provider and patient will vary with nature of the communications involved (i.e. contacting patient with medical history question, referral/consult related communications between providers, etc).

Scheduling/billing information
Appointment, billing, and/or service provider related information may be included as part of targeted communications between health care providers or between health care providers and patients over a secure messaging system such as the one detailed in this PIA. The type of information included will depend entirely upon the nature of the communication involved.

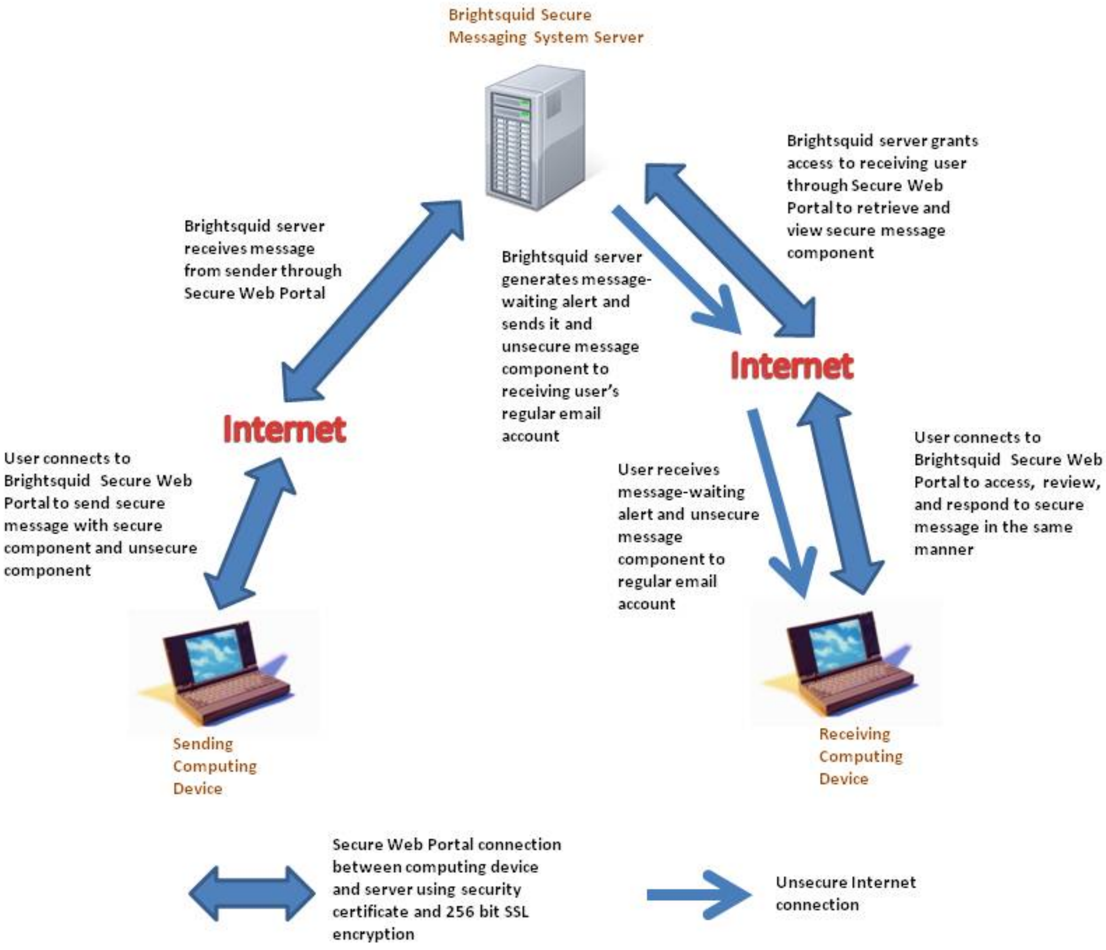
In summary based on the above information, a secure message may include:

| Registration | Diagnostic, Treatment and Care Information | Scheduling / Billing Information |
|---|---|---|
| Patient name**<br>Address<br>Phone number (home)<br>Phone number (work)<br>Additional contact numbers (cell, pager)<br>Sex<br>Date of birth<br>Personal Health Number**<br>Contact name<br>Contact relationship<br>Contact Address<br>Contact phone numbers (home, work)<br>Alerts<br>Pharmacy<br>Chart Number** | Family and social history<br>Past medical history<br>Immunization history<br>Medications<br>Allergies<br>Lab orders and results<br>Problem list<br>Vital Stats<br>Progress notes<br>Consults<br>Diagnostic imaging reports<br>Health service provider information (physician name, provider ID**; referring physician name, referring Dr. ID**) | Appointment date<br>Appointment time<br>Reason for visit<br>Payer<br>Amount owing<br>Units<br>Provider ID**<br>Referring Dr. ID**<br>Service facility<br>Functional centre<br>Date<br>Originating facility<br>Originating location<br>Hospital admit date<br>Comments<br>Pay to entity |

****** Unique identifier

# Project Information Flow Analysis

## Technical Information Flow Diagram


Brightsquid Secure Messaging System Server
Brightsquid server receives message from sender through Secure Web Portal
Brightsquid server generates message-waiting alert and sends it and unsecure message component to receiving user's regular email account
Brightsquid server grants access to receiving user through Secure Web Portal to retrieve and view secure message component
Internet
Internet
User connects to Brightsquid Secure Web Portal to send secure message with secure component and unsecure component
User receives message-waiting alert and unsecure message component to regular email account
User connects to Brightsquid Secure Web Portal to access, review, and respond to secure message in the same manner
Sending Computing Device
Receiving Computing Device
Secure Web Portal connection between computing device and server using security certificate and 256 bit SSL encryption
Unsecure Internet connection

<u>General Technical Information Flow</u>

- User logs into Brightsquid Secure Web Portal linking user to server over a 256-bit encrypted SSL 3.0/TLS 1.2 connection using minimum 8 character strong password with at least one upper case and one number character in it for single factor authentication.
- User creates message to send using contact list or new contact invite dialogue to designate the receiver, filling in secure and unsecure component fields with message parts as appropriate as well as attaching documents for secure viewing if they are part of the message.
- Upon hitting send, the server generates a message-waiting alert and sends it along with any unsecure message component to the receiver's regular email account (or initiates a new user invite to the same regular email account if message is sent to a non-user).
- The receiver upon receipt of the message-waiting alert either initiates the new user dialogue to establish a new account (with birth date as identity verification tool for

patients invited to establish an account), or the receiver as an existing user logs into the Brightsquid Secure Web Portal to link to the server.

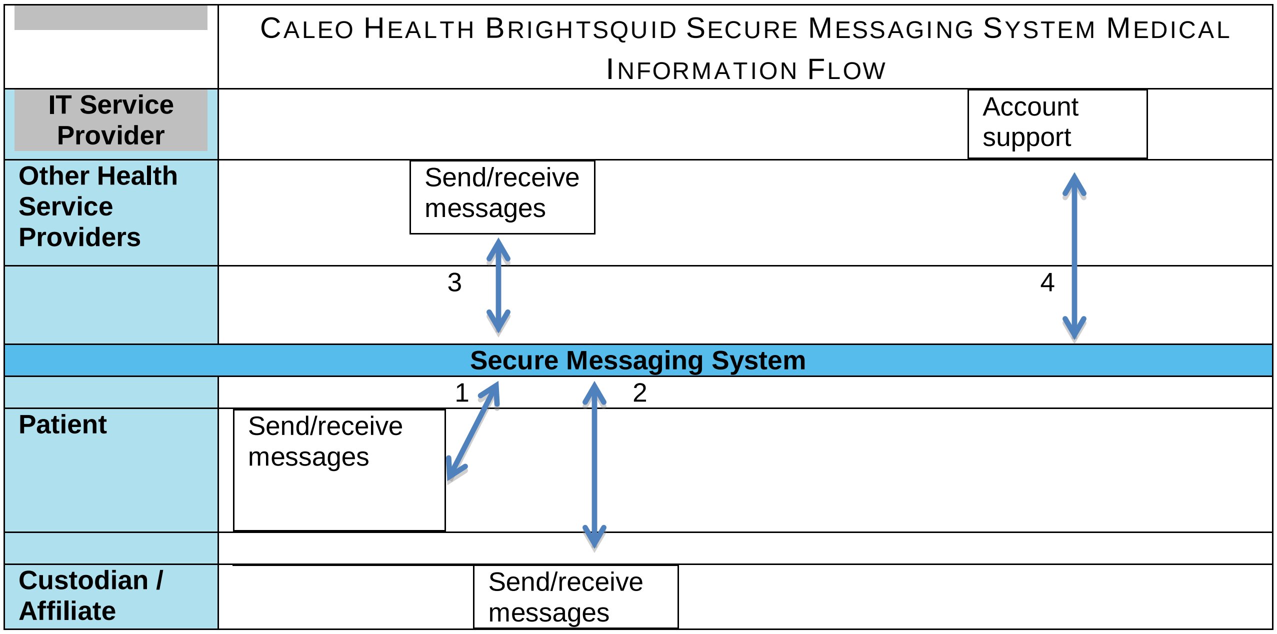
- Once either of the above steps are completed (new user or existing user), the receiver is able to view new messages and their secure contents (message and documents), manage messages, and send responses in the same manner if desired.

**See Section D: Project Privacy Risks and Mitigation for detailed risk assessment and related security/safety measure

## Legal Authority and Purposes Table

The *HIA* permits health care providers to collect, use, and disclose health information with consent, and in specific cases, without consent of the patient whose information is involved (Sections 22, 27, 34, and 35).

Below is our information flow diagram and related authorities for collecting, using, and disclosing information in accordance with the provisions of the *HIA*.



CALEO HEALTH BRIGHTSQUID SECURE MESSAGING SYSTEM MEDICAL INFORMATION FLOW

IT Service Provider

Account support

Other Health Service Providers

Send/receive messages

3

4

Secure Messaging System

1

2

Patient

Send/receive messages

Custodian / Affiliate

Send/receive messages

| Info Flow | Description | Type of Information | Purpose | Legal Authority |
|---|---|---|---|---|
| 1 and 2 | Patient to Custodian – clinic care conversations<br>Collection of health information directly from the patient by custodian except in set circumstances outlined in *HIA*. | Patient Registration, Scheduling, and Diagnostic, Treatment and Care information | **COLLECTION**<br>Providing health services to the patient and related purposes in accordance with *HIA*<br>**USE**<br>Providing health services to the | *HIA* sections. 20, 22, 24, 27, 28, 34, 35, 36, 43 |

| | | | | |
|---|---|---|---|---|
| | Health information is shared with the patient as part of communications – test results, diagnosis, care instructions, appointment scheduling, etc. | | patient and related purposes in accordance with *HIA*<br>**DISCLOSURE**<br>Providing health services to the patient and related purposes in accordance with *HIA* | |
| 2 and 3 | Custodian to Custodian (possibly sent or received by representative affiliate for either) – clinic care conversations<br>Patient information shared with or without consent as appropriate to purpose of conversation | Patient Registration, Scheduling, and Diagnostic, Treatment and Care information | **COLLECTION**<br>Providing health services to the patient and related purposes in accordance with *HIA*<br>**USE**<br>Providing health services to the patient and related purposes in accordance with *HIA*<br>**DISCLOSURE**<br>Providing health services to the patient and related purposes in accordance with *HIA* | *HIA* sections. 20, 22, 24, 27, 28, 34, 35, 36, 43 |
| 4 | Custodian to System Service Provider Support and Help Desk | User account registration information – user identity/name and email address | **USE**<br>Technical support to user accounts | *HIA* section 60 |

## Project Notice

Our clinic recognizes that it is the right of the participant to be advised of purpose for which our clinic collects individually identifying health information from them along with under what legal authority it is collected and who the participant can contact with additional questions or concerns.

While this principle extends to any communications with patients, it is not a requirement or obligation of the secure messaging system to provide this notice.  Instead, it is the responsibility of the custodians and their affiliates to advise patients as needed on purpose of collection, use, and/or disclosure as part of communications with patients whether that be in-person or using a communications system such as telephone, fax, or Internet. This principle extends to both information collected to enable communications and to the communications themselves.

This obligation is tempered with an expectation of reasonableness to all notification requirements. As part of collecting information to enable communications, in this case patient email address to enable messaging, the custodians and their affiliates are reasonably expected to advise the patient that this information is being requested to enable, with their consent, such communications and that they can refuse to participate if they wish and to opt out of such communications at any time.  This notice is provided at time of email address collection either verbally or as part of patient intake forms (as appropriate).

Notification as part of actual communications is only required to the extent to advise the patient receiving a communication (over a reasonably secure means such as the secure messaging system) as to the purpose the custodian or their representative affiliate may be requesting in the communication for the patient to provide specific information. This is expected to take place where and when a custodian or affiliate can reasonably expect that the purpose is not already reasonably inferred by or known to the patient due to the nature of the communication (i.e. if the message is part of an ongoing conversation on a specific topic, negating any necessity to repeat the same notification in subsequent communications after the first).

## Project Consent and Expressed Wishes

Health information shall only be used and disclosed for the purpose for which it was collected, unless alternate use or disclosure is authorized or required by law, or with the knowledge and ***consent*** of the subject individual.

As detailed in this PIA submission, information is only collected, used, and disclosed in accordance with these principles and purposes as allowed by the relevant sections of the *HIA* and its subordinate legislation.

There is no legislative obligation for a system such as the secure messaging system detailed in this PIA submission to specifically account for patient consent and expressed wishes. Instead, these measures are the responsibility of the users (custodians and their representative affiliates) in sending and receiving communications with other health care providers and patients. Our clinic understands and complies with these obligations in accordance with the information already provided in our existing PIA submission covering these topics.

## Project Data Matching and Data Linking

*Data matching* is defined under the *HIA* [s.1(1)(g)] as meaning "the creation of individually identifying information by combining individually identifying or non-identifying health information or other information from 2 or more electronic databases, **without the consent of the individuals** who are the subject of the information."

*Data matching* is not done in using the secure messaging system for patient and health care provider communications.

The use of the secure messaging system for communications does potentially involve data linking. The information present in communications, if it represents identifying health information necessary to provide health care or meet other requirements as permitted in the *HIA,* may require appending to the patient chart to ensure that information is not lost and remains available for those purposes.

## Contracts and Agreements

Within our clinic, confidentiality and security of information are addressed as part of the conditions of employment or service in the clinic (in the case of contract staff, volunteers, and medical students) through training on clinic privacy policies and signing of a confidentiality agreement with the clinic and its custodians (as per our current privacy policies that are detailed in our existing PIA submission).

Service agreements between the vendor and custodians and affiliates are addressed through the user acceptance of vendor terms of use and privacy and security policies when they sign up to use the system as either a subscriber or subordinate user (affiliate or patient). These terms and policies upon review are reasonably compliant with the expectations as laid out in Sections 7.2 and 8.4 of the *HIA Regulation* for an Information Manager Agreement or equivalent.

## Lawful Disclosure and Use of Health Information Outside Alberta

This project and the information it collects is both hosted and used within Canada. The users within our clinic are based in and practice health care within Alberta. The data hosting service for the system is located at a Tier 2 data centre in Markham, Ontario.

System users are conceivably able to communicate using the system with users and non-users anywhere within the world. It is the responsibility of users (custodians and their representative affiliates) to only send communications to other persons authorized in accordance with patient consent and/or the *HIA* for the purposes outlined within the *HIA* when patient health information is involved in those communications including for continuing care that may occur outside the legislative jurisdiction of Alberta.

Our clinic understands that custodians involved are required to protect the information involved from unauthorized use and disclosure in any jurisdiction outside of Alberta to the same extent as would be required by regulation if it was hosted or used in Alberta. And we further understand that failure to take all reasonable steps to ensure this could constitute breach of our obligations under the *HIA*. We believe the privacy and security measures and related vendor policies as outlined in this update PIA submission have reasonably met this requirement.

Finally, Caleo Health is aware that the *Health Information Act s35(1)(i)* gives explicit direction to custodians that they must only disclose health information in response to a subpoena, warrant or order issues or made by a court, person or body having jurisdiction in Alberta (i.e. do not disclose to foreign court orders without proper jurisdiction). When considering responding to a foreign subpoena or other court order, the organization will take all reasonable steps to ensure it has been recognized by a court with jurisdiction in Alberta (including applicable Federal courts), or failing that test, will only disclose the requested health information if consent is received directly from the patient involved or their authorized representative. *(OIPC Investigation Report H2009-IR-002).*

# Section D: Project Privacy Risks and Mitigation

## Access and Security Controls

### Access to Brightsquid Secure Messaging System

Security for devices used to access the secure messaging system from both in-clinic and outside (desktop or mobile device) remains the responsibility of custodians and staff in accordance with the clinic privacy and security policies as reported in our existing PIA submission. These measures can, as appropriate to device and situation, include but are not restricted to system password-protected lockouts and screen savers, physical security of devices, encryption, user account access controls, and remote device wiping capabilities.

The following measures are employed by the vendor or clinic in conjunction with the vendor for security on the hardware, accounts, and connections that are part of the secure messaging system.

Web Portal Interface

The system Web-portal interface, as set up by the vendor, includes the following security and safety measures:

- The Web portal login page and main interface connect with the user's Web browser using a 256-bit encrypted connection using SSL 3.0/TLS 1.2 compliant protocols and specifications. This connection is evidenced to users in the form of a HTTPS designation at the header of the Web page address shown in the browser. This provides for end-to-end encryption of data in motion between the user's Web browser and the system's servers.
- Login to the Web portal requires use of a strong password with a minimum of 8 characters including one upper case character, and one number. This requirement is enforced by system settings.  The system provides a basic prevention of same password re-use only. Password management beyond this level is the responsibility of the user in accordance with clinic policies and procedures, not the system.
- The Web portal interface as part of the login page and main user interface page provides links to company terms of use and privacy and security statements for users to view as needed.
- The unsecure message field includes reminders on appropriate information to use in that field as an additional measure beyond training to help prevent misuse and wrongful disclosure of information outside a secure environment.
- The interface provides reminders to users to verify contact information before sending a message to help prevent wrongful disclosure of information to the wrong recipient.
- The system Web interface has a built-in 60 minute timeout of logins in addition to any in-clinic system protection measures such as locked screen saver timeouts that may be present.

System Hardware, Software, and Data

The system's hardware, applications, and data are hosted out of a third-party Tier 2 data centre located in Markham, Ontario.  Related hardware, software, and data security measures include:

- The hosting service chosen is located within Canada to limit risk of exposure of data to non-Canadian court orders targeting the data centre for action.
- The system database containing user message information is encrypted at rest such that it is not accessible by the vendor company through company system administration tools or by third parties accessing the database directly over Internet connections or onsite where the hardware resides. Instead it can only be access by the relevant user account.
- The database developer can access the database's raw data upon company proper authorization, and the database cannot be accessed without it. This access is only granted for database-related troubleshooting or upgrading events. Further, these access events are monitored by an independent access audit log system that is monitored by company management.
- The data centre provides hardware and software intrusion detection and prevention measures and malware detection and prevention measures to guard against unauthorized access through external Internet connections into the data centre.
- Vendor access to the data centre from company offices for system administration and management occur over a 128 bit encrypted VPN connection dedicated to use by the vendor only.
- The data centre provides biometric access controls, security alarms, video monitoring of access points, hardware access controls, data room and hardware access audit logging, fire detection and suppression, controlled ventilation, and backup power supplies to limit the risk of physical threats and damage.
- The hardware as set up by the data centre on behalf of the vendor to limit system downtime and inaccessibility include redundant servers, redundant drive arrays, and redundant Internet connections. Further, the system is backed up to both onsite and offsite drives with offsite backups to an alternate data centre site being done over an encrypted connection and the offsite backup itself being encrypted. Finally, the current setup is scalable at the vendor's discretion to respond to increased user traffic, and the vendor is investigating with the data centre setting up redundant server/drive arrays offsite as a further system reliability measure.
- The data centre is contracted as the vendor's IT support provider for the hardware, software, and data hosted there with responsibility to maintain and replace components as required in a timely manner as well as assist the vendor in reloading software and data from backups if required as part of restoration services. The vendor has appropriate confidentiality and service agreements in place with the data centre and receives regular reports on hardware access and services carried out by the data centre on behalf of the vendor.

### System Accounts and Administration

User accounts and account administration is protected by the following security measures:

- User account creation requires either application through an online Web page to the vendor for an account or an invite from an existing user. This limits the risk of false user accounts being set up to troll for personal information. Such a risk is still possible, but only with direct existing user or vendor involvement.
- User account creation for patient invitees includes a birth date based validation step (info entered initially by the user sending the invitation) to help ensure the right person is accepting the invitation. Health care provider validation is at the sending user end with a reasonable assumption that the sending user sources the correct contact information for

the health care provider in accordance with their local privacy and security policies with the same due diligence as sourcing correct phone or fax numbers for health care providers that health information is to be sent to.

- The sign up process for an account leads the user through an acknowledgement of terms of use and vendor privacy and security measures statements step to ensure user awareness of proper use of the secure messaging system.  These same statements remain available to users as links from the login and main interface Web pages.
- User accounts require use of a strong password by system design including 8 characters with at least one number and one upper case character.
- All user accounts can access contact lists where profiles are maintained by the specific user associated with the contact including own responsibility for maintaining their contact information. If the regular email address is incorrect or outdated, only the unclassified portion of the message (if any) and message-waiting alert go to the outdated regular email account. Sensitive information and documents still require a valid secure message system user account login to access.
- The Web-based nature of the interface limits the risk of health information being resident on the device used to access the secure message system Web portal (though security of these devices and related Web browsers remains the responsibility of the user, not the vendor).
- Documents being downloaded from the Web portal interface to local computers trigger a reminder alert to store sensitive information properly before the actual download commences. This measure, working in conjunction with clinic policies and procedures, limits the risk of users forgetting to take appropriate health information security precautions for local file storage.
- The main interface Web page includes a variety of reminder notices or flags for each part of the interface including the unsecure message field, regular email address field, and document attachment/download function. The vendor regularly updates the interface for reasonable improvements to information safety and security measures with due regard for interface functionality with different devices and screen sizes.
- User account held information is backed up and retained along with related audit logs tracking usage for 10 years minimum.  User account data is no longer retained and all data is destroyed, including backups, upon deliberate account deactivation by the vendor on user request in accordance with agreements and legislative obligations that information managers not retain health information past the end of the relationship with the users/custodians (as appropriate to circumstance).  The user and/or clinic/custodians are offered the chance to have data in affected user accounts securely transferred to them before such destruction takes place.  Destruction of data is done through use of technical means such as multiple overwriting of data sectors and physical means such as degaussing or destruction of devices, as appropriate to the situation. Audit logs are not destroyed and are retained for the full period as specified above.

## Privacy Risk Assessment and Mitigation Plans

Risk can be mitigated through the deployment of controls which will lessen either the likelihood or consequence of a privacy breach.  In addition to mitigating risk, an organization can choose to avoid the risk by not undertaking the activity, transfer the risk to another entity or accept the risk.

Our clinic-wide *Risk Assessment Table* is as included with our existing PIA submission.

The system *Risk Assessment Table* included with this update PIA submission identifies the risks associated with both the privacy and security of health information held by our clinic *(see Section E - Attachment 4:  Risk Assessment Table)*. Privacy risks cover areas such as health information collection, use, disclosure, retention, access, accuracy and governance. Security risks cover areas such as confidentiality, integrity and availability.  The risk assessment product score reflects the risk level without any mitigation measures.

The risks are grouped into eight causes:

- Unauthorized internal access
- Unauthorized external access
- Unauthorized use of information
- Data modification
- Unauthorized destruction, unintended loss, and unavailability of data
- Physical damage / theft
- Retention and disposition of data
- Contracted third parties

**Reference:** Section E - *Attachment 1: Brightsquid Secure Messaging System Risk Assessment Table*

## System Risk Management Requirements - Gap Analysis

There is no gap analysis for this project as there is no provincially recognized specification set for such a system as there is currently for EMR systems.  All system and capabilities data is as per Section A, C, and D system descriptions in this update PIA submission.

## Monitoring

The clinic's Privacy Officer is responsible for information privacy and security, including ensuring that appropriate administrative, technical and physical security features are in place to protect health information both in-clinic and with contract service providers through the appropriate agreements based on the type of vendor or service provider involved.

All violations or suspected violations of privacy and security must be reported to the Privacy Officer immediately. Contract services providers are obligated to follow the same step as identified in their IMA or equivalent agreements with the custodians. Affected custodians will be involved and consulted with as necessary depending on the level of gravity of the breach / violation.

## PIA Compliance

The *HIA* section 62(1) requires custodians to identify a contact person who is responsible for ensuring compliance with the Act.  Our clinic Privacy Officer is still the same as per our existing PIA submission.

The responsibilities of the organization Privacy Officer are as outlined in our existing PIA submission.

# Section E - Policy and Procedure Attachments

## General Privacy Policies

Our organization’s general privacy policies are as outlined in our existing PIA submission.

## Attachment 1: Brightsquid Secure Messaging System Risk Assessment Table

## Attachment 2: Brightsquid Secure Messaging System Interface Screen Shot

## Caleo Health – Risk Assessment Table for Brightsquid Secure Messaging System

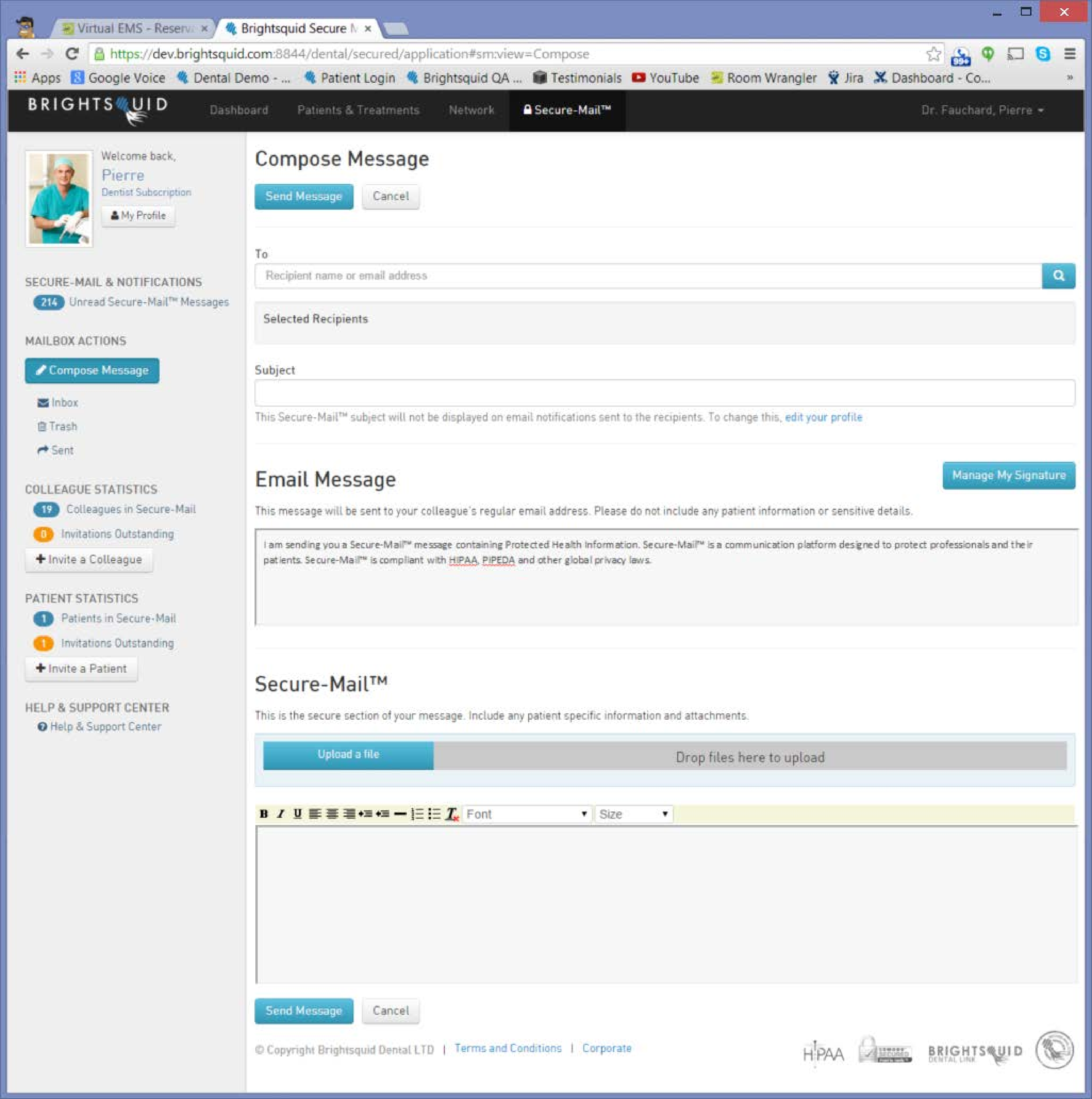
| RISK | PROB. | SEVER. | DISCUSSION & MITIGATION STRATEGIES |
|---|---|---|---|
| **Unauthorized Internal Access**<br>Unauthorized access to patient information by internal personnel, from within facility or through intentional remote terminals. | **Low** | **Med** | One of the inherent risks to medical information is that its access and exposure can be highly revealing. Whereas de-identification might otherwise be a mitigating strategy, patient identification is often embedded directly in records or files, as a precaution against medical mistakes or through the nature of the medical condition and treatment resulting.<br>In the secure messaging system case, identification embedding has the added dimension of potentially being included in both the addressing and body of the message being sent.<br>The primary risk of unauthorized access by internal personnel is focused on access to user accounts. If a user grants another person access to their user account or accidentally leaves it logged in so another user can come in behind them to use the account or view information within the account, this can be considered to constitute a breach of patient health information.<br>Risks of unauthorized internal access are mitigated by the clinic by first ensuring each person authorized to send or manage communications as custodians or responsible affiliates of same have their own user account. The risk is further mitigated by ensuring proper clinic-wide training to users on appropriate safeguard measures including password protection, password change, user account logout upon completion of task, and similar steps.<br>The risks are further mitigated by vendor system measures limiting pathways to how accounts can be established, the fact that other users including custodians can see who has user accounts within their organizational group through the contact list, system timeout, proper use guidelines and reminders, and other such steps. |

| RISK | PROB. | SEVER. | DISCUSSION & MITIGATION STRATEGIES |
|---|---|---|---|
| **Unauthorized External Access**<br>Unauthorized access or disclosure to external party (on or off premises). | **Low** | **Med** | Exposure of personal information from outside the clinic is limited to risk routes through user account compromise, physical compromise of data centre/system security measures, and mis-sending of information to the wrong recipient.<br>User account misuse can result from poor account identity and password protection, leaving the account logged on or logging on in a non-secure network or usage environment (i.e. laptop used on open network and/or left unattended in coffee shop), or sharing of account information with non-clinic persons. This risk is mitigated through clinic privacy and security policies and user training on same.<br>Data centre/system security measures can be compromised by hacking attempts to the system if the hacking entity is determined enough and has tools and approaches not anticipated by and able to get around current security and safety measures as employed by the vendor and data centre. This risk is reasonably mitigated by both the vendor and data centre maintaining an ongoing program of reviewing developing risk/threat vectors and scenarios and regularly updating security and safety measures to account for same in accordance with IT industry security best practices.<br>The mis-sending of communications (and thus potentially health information) to the wrong recipient can occur in the same manner as fax messages can go to the wrong recipient. Measures to mitigate this risk include in-system reminders to verify addresses before sending messages, and regular re-confirming of addresses with health service providers and patients in accordance with clinic privacy and security policies. |
| **Unauthorized Use of Information**<br>Risk of improper use of patient information that has been otherwise legitimately collected and retained. | **Low** | **Med** | This risk is a secondary concern as it flows out from the preceding two risks (unauthorized internal or external access/disclosure). As such, it is mitigated by the same measures.<br>One additional concern is misuse of information by the same persons in the above risk scenarios if they are not complying with expectations of proper use |

| RISK | PROB. | SEVER. | DISCUSSION & MITIGATION STRATEGIES |
|---|---|---|---|
| | | | of health information as outlined in their obligations to the custodian. This risk is mitigated for internal staff and contractors by in-clinic training on privacy and security including related policies and procedures and signing of a confidentiality oath with custodians. This risk is mitigated for external persons such as vendor staff through appropriate service agreements and vendor privacy and security training and policies. |
| **Data Modification**<br>Risk of unauthorized modification of patient health information. | **Low** | **Low** | There is minimal risk of data modification as messages sent are recorded by user accounts and audit logs accordingly.  Users can only delete, archive to folders, or reply to messages, not modify their contents once sent.<br>This risk does not account for deliberate modification of data outside the system's borders including failure to input information accurately into the messaging system or failure to copy information accurately from the messaging system to external records. Those risks are the responsibility of the clinic and custodians and lie outside the scope of this project to mitigate. |
| **Unauthorized Destruction, Unintended Loss, & Unavailability of Data**<br>Interruption to normal operation (e.g., infrastructure failure, system error) can mean that information is not available. More drastic are the risks of permanent damage to data integrity and outright loss. | **Low** | **Low** | There are two primary risk vectors for this category, improper deletion of messages by users before information has been properly transferred to a more permanent record set (i.e. chart) or loss of access to systems due to data centre accident/incident including hacking, physical threats, and technical threats.<br>This risk is mitigated through system and data centre protection and redundancy measures including redundant servers, drives, and power supplies, data centre physical and technical security and safety steps, onsite and offsite data and system backup steps, and vendor disaster recovery plans. |
| **Physical Damage / Theft**<br>Risk to system infrastructure due to man-made or natural hazards such as, flood, power | **Low** | **Low** | Physical theft and damage risks are isolated to in-office equipment and data centre equipment.  Theft of in-clinic equipment used to access user accounts and possibly download health information from messages to the same are the |

| RISK | PROB. | SEVER. | DISCUSSION & MITIGATION STRATEGIES |
|---|---|---|---|
| outage and sabotage. | | | responsibility of the clinic as covered in the clinic's existing PIA submission and are outside the scope of this project PIA.<br>Physical theft of vendor office equipment used to manage the system presents minimal risk to custodians and health information as vendor system administrators have no direct access to health information in user accounts.<br>Physical theft or damage to data centre equipment is of limited risk due to the large array of measures in-place including physical security barriers, video surveillance, biometric and card ID access controls, hardware locks, and audit logs monitoring these measures. Physical damage risk due to accident/incident is limited by similar measures, fire detection and suppression measures, backup power supplies, and adequate ventilation.<br>Technical damage risks from hackers and intrusion are limited by robust and regularly updated technical security measures including intrusion prevention devices, firewalls, malware detection and protection software, etc.<br>Impacts of damage or theft are further mitigated by ensuring redundant hardware and onsite and offsite system and data backup services are in-place. |
| **Retention and Disposition of Data**<br>Retained and archived information is at risk for unauthorized access, disclosure and loss, including inappropriate asset handling at redeployment, sale or destruction. | **Low** | **Low** | Risks associated include loss of user accounts through technical or physical damage, deletion of accounts or information within them, and improper disposal of information deleted on hardware storage devices.<br>Mitigating measures to ensure retention include redundant drives as part of the overall system configuration and onsite and offsite data backups with a 10 year retention of backed up information (or until such time as custodian/vendor relationship is terminated).<br>Deleted information is able to be recovered by system administrators through the backups as well by restoring a user account to a previous save point with system administrator controls to ensure newer data since the restoration point |

| RISK | PROB. | SEVER. | DISCUSSION & MITIGATION STRATEGIES |
|---|---|---|---|
| | | | isn’t lost in the process (i.e. data merger).<br>Improper information destruction is prevented by vendor and data centre policies and procedures governing steps to be followed in deleting accounts and information post-relationship including offering the customer copies of data to be destroyed before any such permanent action takes place. These same policies and procedures also govern proper disposal of storage media that is retired or replaced due to failure of same. |
| **Contracted Third Parties**<br>Risks associated with access and disclosures to contracted third parties. | **Low** | **High** | Associated risks include improper collection, use, storage, and disclosure of information in the hands of contracted third parties involved in the secure messaging system including vendor staff and contracted data centre staff.<br>Improper conduct of vendor staff risks are mitigated by company privacy and security policies and procedures, related training, and audit trails to actions taken. This is further mitigated by the fact that system administrators have no access to user account data and user accounts have audit log trails tracking actions within the accounts.<br>Access by company database developers presents a greater risk due to their ability to access raw user data within the database. This risk is mitigated by the limited number of people acting in this role and the fact that developer access to the database is tracked by an independent audit log system that the developer has no access to; only management does.<br>Data centre personnel wrongful activity risks are mitigated as detailed in previous risk categories concerning data centre administrative, technical, and physical safety and security measures including appropriate agreements with obligations spelt out between data centre and vendor for same. This risk is further mitigated by the fact that the database is encrypted at rest, and communications between the database and user Web browsers is encrypted in motion. |



Welcome back,

Pierre

Dentist Subscription

SECURE-MAIL & NOTIFICATIONS

214 Unread Secure-Mail™ Messages

MAILBOX ACTIONS

COLLEAGUE STATISTICS

19 Colleagues in Secure-Mail

0 Invitations Outstanding

PATIENT STATISTICS

1 Patients in Secure-Mail

1 Invitations Outstanding

HELP & SUPPORT CENTER

## Compose Message

To

Recipient name or email address

Selected Recipients

Subject

This Secure-Mail™ subject will not be displayed on email notifications sent to the recipients. To change this, edit your profile

## Email Message

This message will be sent to your colleague's regular email address. Please do not include any patient information or sensitive details.

I am sending you a Secure-Mail™ message containing Protected Health Information. Secure-Mail™ is a communication platform designed to protect professionals and the ir patients. Secure-Mail™ is compliant with HIPAA, PIPEDA and other global privacy laws.

## Secure-Mail™

This is the secure section of your message. Include any patient specific information and attachments.

© Copyright Brightsquid Dental LTD | Terms and Conditions | Corporate